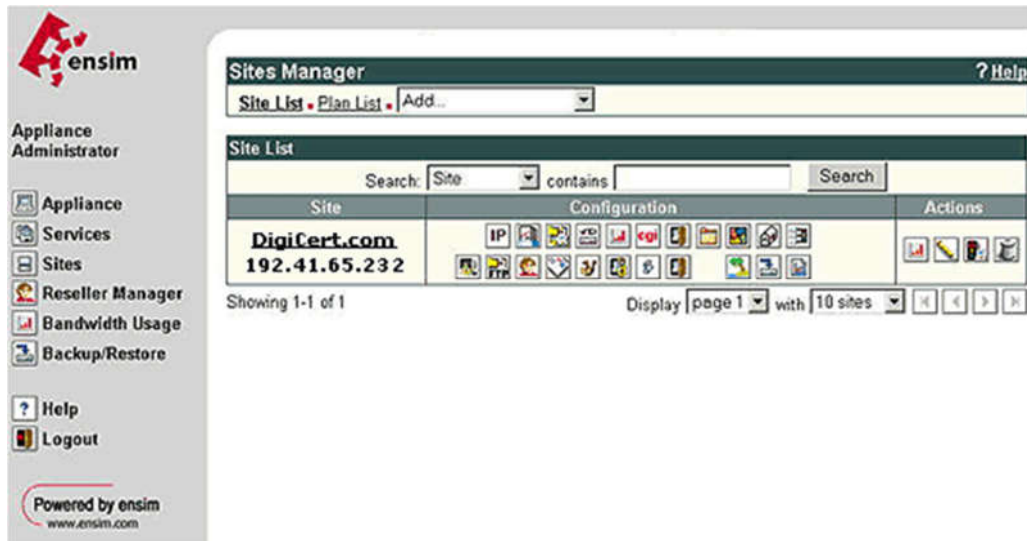


CSR Creation and Installation for Apache using Ensim Control Panel

How to generate a CSR in Apache Ensim Web Server

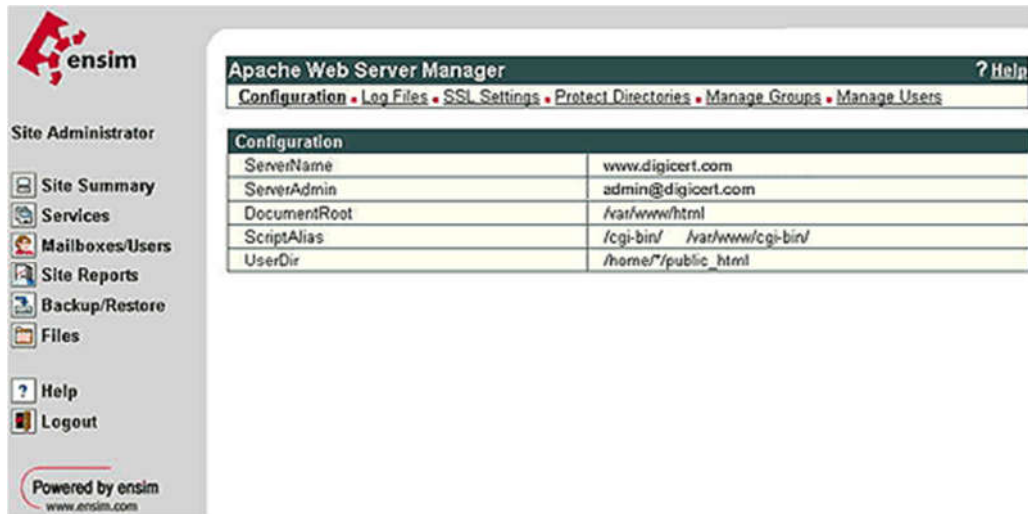
1. Ensim makes the request process easy on the Apache user. First, log in to the Site Administrator and select which site you want to manage, then click on Services.



2. Click on the Actions box next Apache Web Server (at or near the top of the services list.)



3. Then choose SSL Settings from the Apache Web Server Manager.



ensim

Site Administrator

- Site Summary
- Services
- Mailboxes/Users
- Site Reports
- Backup/Restore
- Files
- Help
- Logout

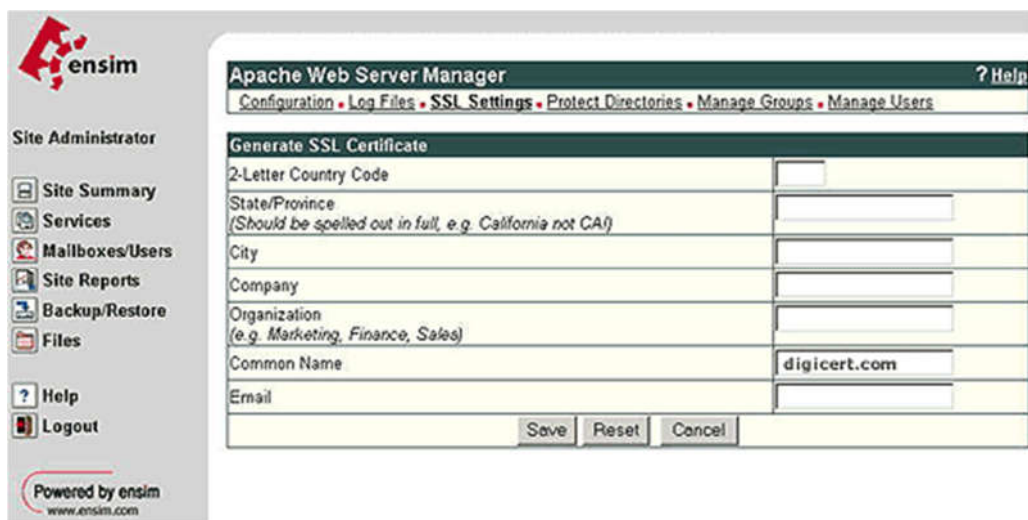
Powered by ensim
www.ensim.com

Apache Web Server Manager ? Help

[Configuration](#) • [Log Files](#) • [SSL Settings](#) • [Protect Directories](#) • [Manage Groups](#) • [Manage Users](#)

Configuration	
ServerName	www.digicert.com
ServerAdmin	admin@digicert.com
DocumentRoot	/var/www/html
ScriptAlias	/cgi-bin/ /var/www/cgi-bin/
UserDir	/home/*/public_html

- Click on Generate. You will be prompted for information about your business and your server -- your Common Name will be entered automatically. Then click on Save.



ensim

Site Administrator

- Site Summary
- Services
- Mailboxes/Users
- Site Reports
- Backup/Restore
- Files
- Help
- Logout

Powered by ensim
www.ensim.com

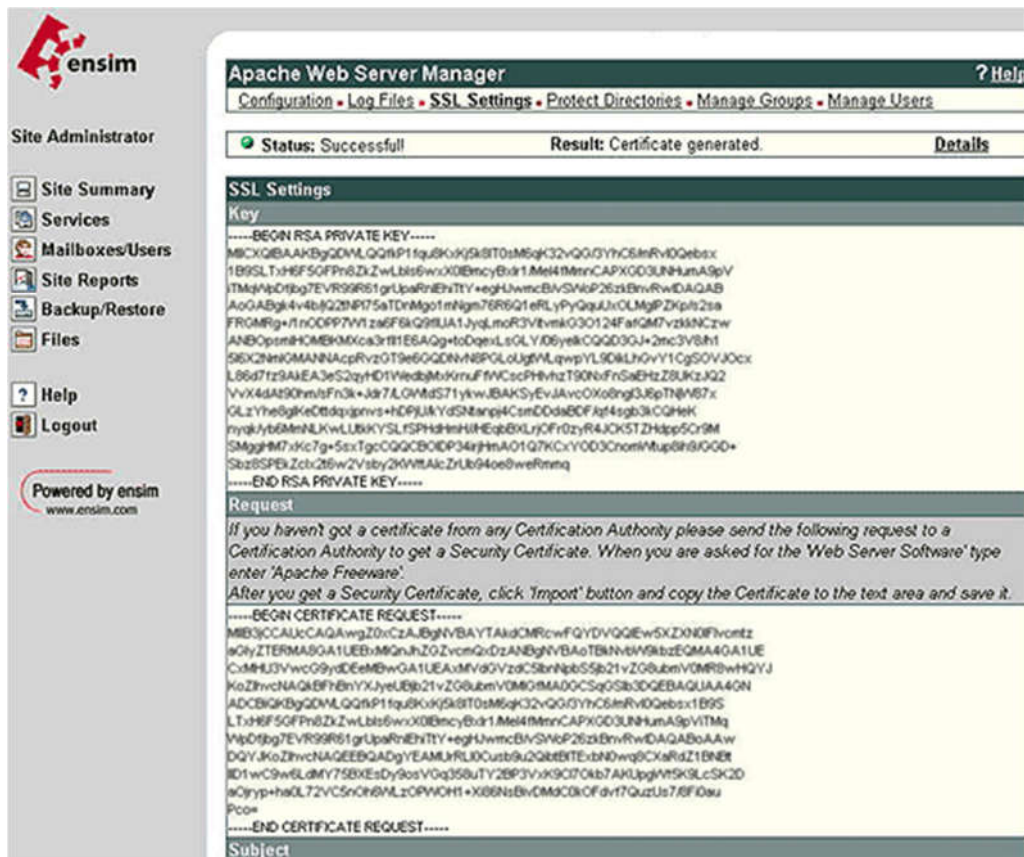
Apache Web Server Manager ? Help

[Configuration](#) • [Log Files](#) • [SSL Settings](#) • [Protect Directories](#) • [Manage Groups](#) • [Manage Users](#)

Generate SSL Certificate




2-Letter Country Code	<input type="text"/>
State/Province (Should be spelled out in full, e.g. California not CA)	<input type="text"/>
City	<input type="text"/>
Company	<input type="text"/>
Organization (e.g. Marketing, Finance, Sales)	<input type="text"/>
Common Name	digicert.com
Email	<input type="text"/>

- This will generate the CSR and the RSA Key, both of which are necessary for the installation of your certificate.



Site Administrator

Site Summary

 Services Mailboxes/Users **Site Reports** **Backup/Restore** **Files**

 Help

 Logout

Powered by ensim
www.ensim.com

Apache Web Server Manager

[? Help](#)

[Configuration](#) • [Log Files](#) • [SSL Settings](#) • [Protect Directories](#) • [Manage Groups](#) • [Manage Users](#)

Status: Successfull

Result: Certificate generated.

Details

SSL Settings

Key

-----BEGIN RSA PRIVATE KEY-----

HXZUEBAABQZDNYCQZMPltqsbqzrTosbmgZvZvGqVYUJYUJmYVQeexs
 iBPSLTHF5SOFPlm7p1Bq5v9x00BncyBd1M4HmEmCAPHXQJUNHAm
 iTMpApk4v7bG2FN9R6r1gTaTmGm1T7eqHwmcVBSAP62z5ImBvZDAQAB
 0oAGABq4v7bG2FN9R6r1gTaTmGm1T7eqHwmcVBSAP62z5ImBvZDAQAB
 FROMIRg1h0COPF7Y1z6ZF6AG2BUA1JyqJm0x0Ydys0L3Y0d6yKQ24F0G3Y
 ANOPsmHmCBKMXKz3r1E8EAQo1JyqJm0x0Ydys0L3Y0d6yKQ24F0G3Y
 56K2nHGMANNACSpv2G196vGGDNHmBPGLQJdHvYUJ90dLhVYUJG1Y
 LB6d7z3AIEA3e3p2Y01ViedmK0mHvFncSpHvhdY90dLhVYUJG1Y
 Yv4A49A9m0F7nK3Jd7L0AM571ykwJBKASyEvJAwKz3r1E8EAQo1JyqJm0x0Ydys0L3Y0d6yKQ24F0G3Y
 GLZYh5gKcBtdsqjv5+HdFJYUJdSMnq4CsmD0dAB0F4f4s3g3CQHk
 nyk4v7b6mKULWUBK9YLSPrdHmYEqBdKJr0fzyRAJ3KZ5hdpsC9r5M
 SMggmP7Xc7g5v7xTcCQCB0ECP34jrHAm01G7KCY0D3CnrmMup8BKGQD+
 Sz3SPEBZ3Zc26wZ5v2zWNAKcZUW4K0d4ewfwmn

Request

If you haven't got a certificate from any Certification Authority please send the following request to a Certification Authority to get a Security Certificate. When you are asked for the 'Web Server Software' type enter 'Apache Freeware'.

After you get a Security Certificate, click 'Import' button and copy the Certificate to the text area and save it.

-----BEGIN CERTIFICATE REQUEST-----

MB3GCACACAGAAWt2CzA2BgNBAYTAAGCMFwVQDyVQGGvSXZG8AFvmtz
 zTETRMAD9A1UEBmQnJhZQZvcmZkZQAnBgNABATBNvWkSbZQ8MA4A1UE
 CdMhJ3Vwv9gYdEeBmGA1UEAUA1Mv9VZ2t58nBpZS52b1ZG0ubVQMRWbHQ
 KQzhvncAAGBFbFhYJyeUeU2b1ZG0ubVQMRMA0DCCSgZG0uBQAUA4A2N
 ADCBQBgZG0MLGQnqP1fauK3Kj3kBT0tAm6gQzG2vQyJhZC8nRvDQebs1B9S
 LtJhF50FPNDZwLzLtsf0w0D0Bcnyb1M4eMfMnCAPXG03UHhAnAspVITMg
 Vp0p07gvYK9R91gUpRnRhtYt+eghUwBvN9G26zBhWvDwAQA0AAw
 DQYKQzhvncAAGBFbFhYEAUMLRU0C2t02BtFEtzbHwQvCxaRZ1BNB
 1D1wC9w6MLG75BX0e5d0sYVqG35uYtZBP3v93Cf0Kb7AKUqJpW9K9LcSKQ2
 oGyp+haDL72VC5nCh6MLzCPW0H1+X0BnBbVMG3CkCvYt7QutUs7fJf0u
 Pops

-----END CERTIFICATE REQUEST-----

Subject

- Copy the CSR to text file and **submit to us** for our process.

Installing the Primary SSL Certificate file (your_domain_name.crt)

1. To begin, save your certificate into the directory for your SSL Certificates. We will use `/etc/ssl/crt/` as an example. The public and private key files should be in the same directory already. In the example below, the private key will be `private.key`. The public key will be labeled `yourdomainname.crt`. Make this directory readable only by root.
2. Log in to the Administrator console and choose the website you are securing.
3. Click on Services, then click on Actions next to Apache Web Server. Now choose SSL Settings. (A 'Self Signed' certificate should already be saved.)

Installing the Intermediate Certificate file

Ensim currently does not provide a User Interface (UI) to install an Intermediate Root CA Certificate. This installation will need to be completed directly using SFTP or SSH. The Intermediate certificate must be installed on your server before your certificate will be trusted.

1. Locate the Virtual Site File

1. Locate which Virtual Site File you will edit. To do this, go to the following directory on your Ensim Server.

/etc/httpd/conf/virtual

Example of files you might see under the virtual directory (the number of Site Files depends on how many virtual sites you are hosting on your Ensim Server):

site1
site2
site3
etc...

2. Now view each Site File (using an html/text editor) until the Site# File for the site/domain you seek is identified. At that top of the Site Files you will find for example the following information:

<VirtualHost 000.00.00.000:80>

ServerName www.yourdomain.com

3. Once you have identified the Site File you seek please note the number for future reference. You will now edit this same file (see instructions below).

2. Edit the Virtual Site File

1. Now you will Edit your Site File by adding the following line below (this line is bolded). Make sure you replace the site# with the actual virtual site number (example: site1)

</Directory>

SetEnv SITE_ROOT /home/virtual/site#/fst

SetEnv SITE_HTMLROOT /home/virtual/site#/fst/var/www/html

Include /etc/httpd/conf/site#

SSLEngine on

SSLCertificateFile /home/virtual/site#/fst/etc/httpd/conf/ssl.crt/server.crt

SSLCertificateKeyFile /home/virtual/site#/fst/etc/httpd/conf/ssl.key/server.key

SSLCACertificateFile /home/virtual/site#/fst/etc/httpd/conf/ssl.crt/IntermediateCA.crt

</VirtualHost>

< /IfDefine>

2. Copy the Intermediate CA Root Certificate file to the directory where your sever certificate has been saved as in the example above:

/home/virtual/site#/fst/etc/httpd/conf/ssl.crt/IntermediateCA.crt

Again you will need to substitute site#

3. Back up your current Site File.

4. Save your edited Site File.

3. Restart Apache

Once you have copied/uploaded the Intermediate Root file. You will now restart Apache.

Note: The instructions above are for installing your certificate to a site managed through Ensim. If you wish to install the SSL Certificate to Ensim itself rather than a site managed through Ensim, the host configuration is basically the same, but the host configuration file for the Ensim interface is /usr/lib/opcenter/fastcgi/httpd-templ.conf